OPENING STATEMENT OF
LUIS V. GUTIERREZ
RANKING DEMOCRAT
SUBCOMMITTEE ON OVERSIGHT & INVESTIGATIONS AND SUBCOMMITTEE ON FINANCIAL INSTITUTIONS AND CONSUMER CREDIT JOINT HEARING
"FIGHTING FRAUD: IMPROVING INFORMATION SECURITY"
APRIL 3, 2003

Good morning Chairs Kelly and Bachus and members of the committee.

Today, more than ever, identity theft takes a myriad of forms. Modern thieves are utilizing massive digitized databases to access and steal consumers' personal information.

And the number of cases keeps rising. Identity theft is now the number one consumer fraud complaint nationwide. And it has been estimated that the amount of money stolen from consumers could multiply three-fold this year alone.

Identity theft-related losses already exceed $1 billion each year. My home state of Illinois ranks fifth in the nation and Chicago ranks second among cities for identity theft complaints.

As too many people are learning the hard way, identity thieves steal social security, bank account, and credit card numbers and use them to commit fraud, very often destroying the credit rating and financial future of their victims.

Every year, thousands of these victims are left financially ruined, often with severe credit problems and even false criminal records that they must spend years working to erase. Even in minor cases, victims spend countless hours trying to restore their credit rating.

While working arduously to correct their records, thousands of victims are faced with poor credit, which translates into an inability to acquire goods, including being denied the opportunity to purchase a home, a car, appliances, insurance products and the list goes on and on.

These crimes can prove especially difficult for local police and prosecutors to track because thieves use computers, telephone lines and the Internet to cross cities, states and nations.

And so we are gathered here today to discuss ways to help consumers by increasing the security of data that contains our personal information. And to understand some of the possible loopholes that have enabled these cases to occur in the first place, to hear about data security efforts

undertaken by the companies that hold our private information and to look for ways to help consumers have quick and better access to their personal records when identity theft incidents occur.

One of the most fundamental problems is that consumer are very often left out of the loop after their information has been stolen. This is unacceptable. Consumers need better access to their own records and other relevant data to be able to combat these issues.
They also need to be informed in a timely manner that their information has been accessed.

In one of the cases that will be discussed today, a former employee of Teledata Communications Inc. is being charged with the biggest identity theft fraud in U.S. history.

One of the most outrageous aspects of this specific case is that in March of 2000, the alleged perpetrator quit his job with Teledata, but that didn't even slow down his scheme.

The alleged perpetrator only worked at Teledata for 10 months, but the scam continued for nearly three years.

The company security codes he had allegedly stolen still worked and most were accessible right up until his arrest earlier this year.

In the meantime, some 30,000 people had their identities stolen and the financial losses so far have reached more than $2.7 million, although that amount is expected to rise considerably.

How could personal data be so easily accessible?

What kind of safeguards do companies have in place to deter these nefarious practices?

I hope that this hearing will serve as an opportunity to answer some of these pressing questions.

Thank you for holding this important hearing. I look forward to the testimonies.